(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 607 767 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
26.11.1997 Bulletin 1997/48

(51) Int Cl.[6]: **G07F 7/10**, H04M 1/66, H04L 9/32

(21) Application number: **93850205.1**

(22) Date of filing: **29.10.1993**

(54) **Access controlled device for rendering services**

Vorrichtung mit Zugangskontrolle für den Erhalt von Dienstleistungen

Dispositif permettant des services commandés par accès

(84) Designated Contracting States:
DE ES FR GB IT NL SE

(30) Priority: **09.11.1992 SE 9203351**

(43) Date of publication of application:
27.07.1994 Bulletin 1994/30

(73) Proprietor: **ERICSSON INC.**
Research Triangle Park, N.C. 27709 (US)

(72) Inventor: **Barvesten, Mats Olof**
S-222 48 Lund (SE)

(74) Representative: **Mossmark, Anders et al**
Albihn West AB,
Box 142
401 22 Göteborg (SE)

(56) References cited:
EP-A- 0 281 728
EP-A- 0 301 740
EP-A- 0 448 369

EP 0 607 767 B1

Description

TECHNICAL FIELD:

The present invention relates to an arrangement for rendering services as stated in the first part of claim 1.

Such an arrangement is known from document EP-A-0 301 740. Similar devices may under a lot of circumstances easily be abused and are very attractive to steal which might have serious consequences. This is the case as well if e.g. the access units are not lockable or are not locked as well as if the terminal unit is not lockable or is not locked so that they merely can be used by users who really should have access to the one or the other of the units. This is e.g. the case with mobile telephones where the subscription is not related to a particular mobile telephone or terminal unit but is related to a separate card. Therethrough a terminal unit or a telephone may be used with any card. If on the other hand the access unit, or the card, is not locked, anyone may use the card and therethrough also charge the subscription. One way to solve this problem, i.e. to protect the terminal unit as well as the access unit is to implement a "lock" in the terminal unit as well as in the access unit wherethrough a user has to enter a code to "unlock" the terminal unit and a further code to "lock up" the card and thus get access to the subscription. This however is tedious since two different codes have to be entered each time upon use which is very inconvenient, among others since it is difficult to remember the increasing number of codes which are necessary in the society and also because it is annoying each time, which may be a large number of times, having to enter two codes. It is therefore very probable that the user inactivates one or the other of the codes or in the worst case both identification codes in order to be able to get a quick access to his phone whereby the user runs the risk that the device, or one of the units comprised by the device or arrangement, are abused or stolen.

STATE OF THE ART:

Devices as referred to above are known but as mentioned above they suffer from the drawback that either two different codes have to be entered upon every activation of the terminal or it is not bothered to lock e.g. the terminal, but also in some cases, the card or the access unit. This is for example the case with the digital GSM-system. In this system the subscription is on a separate so called SIM-card (Subscriber Identity Module). In this case the terminal unit, or the telephone, is very attractive for stealing since the SIM-card which should have access to the telephone simply can be exchanged through another SIM-card and therethrough the telephone may be used freely by users who should not have access to the, in this case, telephone. This is particularly the case when the terminal units are intended to be used by a particular user or a particular group of users or when the terminal quite simply is stolen. In the he known device the access unit, or the SIM-card, comprises a so called PIN-code (Personal Identification Number) whereas the terminal unit, or the telephone, in turn comprises another PIN-code so that in order to get a full protection of terminal unit (telephone) as well as access unit (card), both codes must be entered at every activation of the terminal unit or the telephone. This leads consequently to a very awkward handling of the device.

On the other hand, in known analogue mobile telephone systems the subscription is programmed into the telephone terminal. This is done with special equipment and is handled by authorized personnel which is picked out and controlled by the operator, therefore the same problems do not arise in this case.

BRIEF DESCRIPTION OF THE INVENTION:

The object of the present invention is to provide an arrangement for rendering services wherein a terminal unit as well as an access unit are safe against thefts and may not easily be abused at the same time as the device is easy to use and in the normal case do not require a double entering of codes and wherein particularly advantageous no entering or giving of codes at all is necessary to give the owner or the prioritized user access to the device without the device therefore getting less safe or protected against thefts. A further object with the invention is to provide an arrangement which permits fast and easy access and wherein the simplified access may be given to one or more users depending on what is desired.

An arrangement through which these as well as other objects are achieved is given by the characteristics of the characterizing part of claim 1.

A further object with the invention is particularly to, if so desired, enable to render information about identification number (for example telephone number) or codes belonging to access units which have been acceded simplified access. This object is achieved through the characteristics as given in claim 12.

Further preferred embodiments are given by the characteristics in the further subclaims.

BRIEF DESCRIPTION OF THE DRAWINGS:

The invention will in the following be further described with reference to the drawings in an explanatory and by no means limiting way, wherein

Fig. 1 schematically illustrates a terminal unit and an access unit in the form of a telephone with a card,

Fig. 2 schematically illustrates an example of a flow diagram with steps which are gone through upon activation of the terminal for "locking up" of terminal unit as well as access unit (in the illustrated case a telephone

and a card).

DETAILED DESCRIPTION OF THE INVENTION:

In the embodiment shown in Fig. 1 a device or an arrangement 10 is shown wherein the terminal unit comprises a mobile telephone 1 and the access unit comprises an electronical card 2 comprising the subscription. The device furthermore comprises a push button means 5, a memory 3 and a micro processor unit 4. In the display 6 among others telephone numbers are shown. In the shown embodiment the device refers to the cellular so called GSM-mobile telephone system, particularly the CME 20-system (Ericsson). In this context it is also referred to recommendation GSM 11.11. In the shown embodiment the card 2 with an electronical memory comprises a so called SIM-card (Subscriber Identity Module) further described in Recommendation GSM 02.17 which contains the information which unambiguously identifies the subscriber. In the SIM-card 2 the so called IMSI-code (International Mobile Subscriber Identity) is stored. A mobile station, MS, which for example may be a station mounted on a vehicle, a portable station or a hand carried station, may only be used if a valid IMSI-code is present. In the cases when the terminal unit or the telephone 1 is not locked or secured by a so called EIR-register (Equipment Identity Register) (not yet in use) which in one way can be seen as a different alternative to the present invention as theft protection is concerned, it would be easy to abuse or steal the terminal unit or the telephone 1. Upon starting up or activation of the telephone 1, the telephone 1 and the SIM-card 2 communicate with each other. The IMSI-code for the SIM-card(-s) 2 is (are) to be stored in a memory in the phone, e.g. in an EEPROM-storage. The IMSI-code may then be stored in a number of different ways which are known per se, e.g. the whole of it, partly, non-ciphered or ciphered or random numbered generated with calculation of rest or any other method. The storing may take place either automatically or manually. According to an advantageous embodiment of the invention it is possible to, apart from storing of the identity of the own SIM-card, i.e. its IMSI-code, also store the IMSI-codes of a number of other SIM-cards which should have a simplified or prioritized access to the terminal unit or the telephone 1.

Particularly under reference to the flow diagram of Fig. 2 in the following the sequence will be described wherein, after one or more IMSI-codes have been stored in a storage of a terminal unit as well as possibly also PIN_t and PIN_c-codes, the terminal is activated or started up wherein a number of different possibilities are possible depending on the actual IMSI-code having been stored or not.

Upon activation of the telephone, wherein either a card already is present in the telephone 1 or a new one has been introduced, the actual $IMSI_c$-code is sent to the telephone 1 (according to the GSM-recommendation) via the microprocessor 4, as stated above, where it is compared to in the telephone 1 stored $IMSI_{s,i}$-code (-s). If $IMSI_c$ corresponds to any $IMSI_s$-code which has been stored in the telephone 1, the telephone is started up without requiring any further measure to be taken or without asking for any further code. If on the other hand the codes do not correspond the telephone 1 demands a PIN_t-code for the terminal unit or the telephone 1.

Thus, on every occasion of activation of the telephone 1, in the memory 3 stored code(-s) ($IMSI_{s,i}$) are compared with the received code ($IMSI_c$) of the actual SIM-card. A so called PIN-code for the SIM-card may likewise be stored in the storage 3 in a way similar to that of the IMSI-code(-s). In the storage 3 of the terminal unit (telephone) are apart from one or more IMSI-codes also a PIN_t, i.e. a Personal Identification Number for the terminal, is stored. According to different embodiments may furthermore PIN_c of those cards whose $IMSI_c$-code (-s) have been stored, be stored therein as well as a telephone number for the corresponding subscription. This is however dependent on desires and requirements and provisions and merely shows advantageous embodiments. Now returning to the case wherein the actual $IMSI_c$-code does correspond to the stored $IMSI_s$-code and the terminal is locked up. Thereafter is investigated if the actual PIN_c-code of the card is stored. If this is the case, the PIN_c-code of the actual card is picked up from the memory 3 whereupon it is transmitted to the card 2 which thereafter is locked up and then the telephone 1 as well as the card (access unit) 2 are unlocked and the device 10 is as far as locking is concerned ready to be used or open for communication. In this case, consequently, is not required the entering of any code by the user. (If PIN_c is stored (and activated), this code is requested and will then have to be entered or given).

If however the actual $IMSI_c$-code does not correspond to any stored $IMSI_s$-code the terminal unit 1 or the telephone 1 requests a PIN_t-code for the terminal. When this code is given the terminal 1 is unlocked. Thereafter is asked if the PIN_c-code for the card is activated. If not, the card is unlocked and thus was not locked. If yes, the PIN_c-code is requested and when this is given, the card is locked up and the device is ready to be used as far as locking is concerned. If on the other hand the actual IMSI-code has corresponded to a stored $IMSI_s$-code it is also possible that the PIN_c-code of the actual card has not been stored. The terminal is in this case, as already mentioned above, already unlocked. Then is examined if any PIN_c-code for the card is activated. If yes, this is given whereupon the card is locked up. If not, the card consequently has not been locked and is therefore unlocked and the device is ready to be used as far as locking is concerned. Thus it is possible for an authorized user, i.e. a user who should have access to telephone as well as to card not to enter any code at all but that the card as well as the terminal are unlocked automatically. If however the actual $IMSI_c$-code has not been stored in the terminal it is possible to

get access by entering PIN-codes for terminal and card. Eventually these codes could be associated with each other and for example consist of one and the same code.

According to a preferred embodiment at least one $IMSI_c$-code as well as also PIN-codes for card as well as for terminal are stored in the memory. To avoid the storage of the PIN-code of the card it might also be possible, as mentioned above, to associate this with the PIN-code of the terminal. According to a preferred embodiment is however the PIN_c-code of the card stored in a ciphered form in the memory 3.

The cards may for example comprise cards with an electronical memory but also cards with a magnetical memory or other alternatives are possible.

According to a preferred embodiment it is possible, in case the $IMSI_c$-code of an actual card is stored in the memory 3 of the terminal 1, to show for example the telephone number of the actual subscription or the SIM-card which can be useful since this in no other way is visible. Then it is examined, after unlocking of the card, if the telephone number of the card is stored in the terminal. If this is the case, it is picked up from the memory and is shown on the display 6. If the telephone number is not stored in the terminal it is examined if the telephone number is stored in the card. If this is the case, the telephone number is picked up from the memory and is also shown on the display 6. If the telephone number is not stored, no display takes place. The display of telephone numbers is advantageous since the telephone number in no other way is visible, neither on the terminal unit or on the card and if a user for example has several cards it may be difficult to remember the number as it often is difficult to remember the own number. This is the case both if one or more telephone numbers is/are connected to stored IMSI-codes.

It is furthermore possible to carry out the storage of different codes (IMSI, PIN) in the memory 3, either manually or automatically. With manual storing it could for example be effected by a so called push button device 5 or similar. Furthermore, it should be possible to change stored codes as well as to delete codes or add codes.

The invention shall of course not be limited to the shown embodiments and does not have to be a mobile telephone but it is related to every device rendering services, e.g. devices for data communication or others comprising a terminal unit and an access unit which e. g. may comprise a subscription or similar and where it is desirable to secure the units forming part of the device against theft and abuse. A device may also comprise more than two units. The invention should not be limited to the shown embodiments but can be freely varied within the scope of the claims.

Claims

1. Arrangement (10) for rendering services such as telephone communication, data communication etc., comprising a terminal unit (1) and an access unit (2), the terminal unit (1) comprising terminal unit identification means (PIN,) being stored in the terminal unit (1) and the access unit (2) comprising first access-unit-identification means (IMSI) in the form of a code or similar, said terminal unit (1) and said access unit (2) being lockable, **characterized** in that, in the terminal unit (1) are furthermore stored first access-unit-identification means ($IMSI_{s,i}$) for a given number (n) of access units (2) (SIM), and that the access unit (2) comprises second access-unit-identification means (PIN_c) which may be activated or inactivated, whereupon starting up of the arrangement involving contact between the terminal unit (1) and an access unit (SIM) (2) with a certain access-unit-identification means ($IMSI_c$), the code of the identification means ($IMSI_c$) of the access unit (2) is compared with in the terminal unit stored code (-s) for access-unit-identification means ($IMSI_{s,i}$), wherein correspondence between said stored first access-unit-identification means ($IMSI_{s.i}$) and actual first access-unit-identification means ($IMSI_c$) leads to locking up of the terminal unit (1), whereas upon non-correspondence between stored and actual first access-unit-identification means, said access unit (2) and said terminal unit (1) are unlocked upon a user providing a code corresponding to said terminal-unit-identification means (PIN_t) and a code corresponding to said second access-unit-identification means (PIN_c), if activated.

2. Arrangement according to claim 1, **characterized** in that said second access-unit-identification means (PIN_c) comprises a code which is given manually by the user.

3. Arrangement according to claim 1, **characterized** in that also second access unit identification means (PIN_c) are stored in the terminal unit (1), the terminal unit upon correspondence between stored and actual access-identification-code ($IMSI_s = IMSI_c$) automatically transferring the second identification means (PIN_c) to the access unit (2) so that the arrangement (10) may be used without the second access unit identification code (PIN_c) having to be given by the user.

4. Arrangement according to claim 1, **characterized** in that if the second access unit identification means (PIN_c) has not been stored and that upon correspondence between in the terminal unit (1) stored first access-unit-identification means ($IMSI_{s,i}$) and the actual access-unit-identification means ($IMSI_c$), the access unit (2) is locked up by entering of (PIN_c).

5. Arrangement according to claim 1, **characterized** in that upon non-correspondence between stored

and actual access-identification code ($IMSI_c \neq IMSI_s$) terminal unit (1) as well as access unit (2) are unlocked by giving one of the terminal identification code (PIN,) or the second access-unit-identification code (PIN_c).

6. Arrangement according to anyone of claims 1, 2 or 4, **characterized** in that upon non-correspondence between actual and any stored access-identification-code ($IMSI_c$) $\neq$ $IMSI_s$) terminal identification code (PIN_t) as well as second access identification code (PIN_c) have to be given.

7. Arrangement according to anyone of the preceding claims, **characterized** in that the terminal unit (1) comprises a mobile telephone.

8. Arrangement according to anyone of the preceding claims, **characterized** in that the access unit (2) comprises a card, e.g. with an electronical or a magnetical memory.

9. Arrangement according to claim 8, **characterized** in that the access unit (2) comprises a SIM-card (Subscriber Identity Module) defining the subscription of the mobile telephone (1).

10. Arrangement according to anyone of the preceding claims, **characterized** in that the first access-unit-identification code ($IMSI_{c,i}$) for at least one subscription which should have access to the telephone unit (1) or the terminal unit is stored in the terminal unit, said identification code for example being stored in a EEPROM-memory in a manner known per se, as a whole, partly, ciphered, random number generated with rest and so on.

11. Arrangement according to claim 10, **characterized** in that furthermore one or several further access-unit-identification codes ($PIN_{c,i}$) are stored in a memory in the terminal unit (1) for example as a whole, partly or ciphered in any per se known way.

12. Arrangement according to claim 11, **characterized** in that at least one second identification code ($PIN_{c,i}$) is stored ciphered in a memory in the terminal unit (1).

13. Arrangement according to any one of the claims 10-12, **characterized** in that the storage of the first access-identification-code ($IMSI_s$) takes place automatically.

14. Arrangement according to any one of claims 10-12, **characterized** in that the storage of the first access-identification-code ($IMSI_s$) takes place manually, for example via a push button device (5) or similar.

15. Arrangement according to any one of the claims 10-14, **characterized** in that at least one second access-identification-code (PIN_c) is stored in a memory in the terminal unit (1) in a way which is essentially analogue to the storing of the first access identification code ($IMSI_s$).

16. Arrangement according to any one of claims 7-15, **characterized** in that at least one to at least one access unit (2) belonging telephone number is stored, either in a terminal storage or in a storage in the card so that this is picked up from said storage and shown on a display (6) when the arrangement (10) is unlocked.

Patentansprüche

1. Vorrichtung (10) für den Erhalt von Dienstleistungen, wie etwa Telefonkommunikation, Datenkommunikation etc., umfassend eine Terminaleinheit (1) und eine Zugangseinheit (2), welche Terminaleinheit (1) eine Terminaleinheits-Identifikationseinrichtung (PIN_t) enthält, die in der Terminaleinheit (1) gespeichert ist, und welche Zugangseinheit (2) eine erste Zugangseinheits-Identifikationseinrichtung (IMSI) in Form eines Codes oder dergleichen enthält, welche Terminaleinheit (1) und Zugangseinheit (2) verriegelbar sind, dadurch gekennzeichnet, daß in der Terminaleinheit (1) ferner eine erste Zugangseinheits-Identifikationseinrichtung ($IMSI_{s,i}$) für eine gegebene Anzahl (n) von Zugangseinheiten (2) (SIM) gespeichert sind und daß die Zugangseinheit (2) eine zweite Zugangseinheits-Identifikationseinrichtung (PIN_c) enthält, die aktiviert oder inaktiviert sein kann, wobei bei Betriebsbeginn der Vorrichtung, was einen Kontakt zwischen der Terminaleinheit (1) und einer Zugangseinheit (SIM) (2) mit einer bestimmten Zugangseinheits-Identifikationseinrichtung ($IMSI_c$) einschließt, der Code der Identifikationseinrichtung ($IMSI_c$) der Zugangseinheit (2) mit einem oder mehreren in der Terminaleinheit (1) gespeicherten Code bzw. Codes für die Zugangseinheits-Identifikationseinrichtung ($IMSI_{s,i}$) verglichen wird, wobei die Übereinstimmung zwischen der gespeicherten ersten Zugangseinheits-Identifikationseinrichtung ($IMSI_{s,i}$) und der tatsächlichen ersten Zugangseinheits-Identifikationseinrichtung ($IMSI_c$) zu einer Verriegelung der Terminaleinheit (1) führt, wohingegen bei Nichtübereinstimmung zwischen der gespeicherten und der tatsächlichen ersten ZugangseinheitsIdentifikationseinrichtung die Zugangseinheit (2) und die Terminaleinheit (1) entriegelt werden, wenn ein Benutzer einen Code eingibt, der der Terminaleinheits-Identifikationseinrichtung (PIN_t) entspricht, und einen Code, der der zweiten Zugangseinheits-Identifikationseinrichtung (PIN_c) entspricht, wenn akti-

viert.

2. Vorrichtung nach Anspruch 1, dadurch gekennzeichnet, daß die zweite Zugangseinheits-Identifikationseinrichtung (PIN_c) einen Code umfaßt, der manuell durch den Benutzer eingegeben wird.

3. Vorrichtunq nach Anspruch 1, dadurch gekennzeichnet, daß auch die zweite Zugangseinheits-Identifikationseinrichtung (PIN_c) in der Terminaleinheit (1) gespeichert ist, wobei die Terminaleinheit bei Übereinstimmung zwischen gespeichertem und tatsächlichem Zugangsidentifikationscode ($IMSI_s = IMSI_c$) automatisch die zweite Identifikationseinrichtung (PIN_c) zu der Zugangseinheit (2) überträgt, so daß die Vorrichtung (10) benutzt werden kann, ohne daß der zweite Zugangseinheits-Identifikationscode (PIN_c) durch den Benutzer eingegeben werden muß.

4. Vorrichtung nach Anspruch 1, dadurch gekennzeichnet, daß dann, wenn die zweite Zugangseinheits-Identifikationseinrichtung (PIN_c) nicht gespeichert wurde, bei Übereinstimmung zwischen der in der Terminaleinheit (1) gespeicherten ersten Zugangseinheits-Identifikationseinrichtung ($IMSI_{s,i}$) und der tatsächlichen Zugangseinheits-Identifikationseinrichtung ($IMSI_c$) die Zugangseinheit (2) durch die Eingabe von (PIN_c) verriegelt wird.

5. Vorrichtung nach Anspruch 1, dadurch gekennzeichnet, daß bei Nichtübereinstimmung zwischen gespeichertem und tatsächlichem Zugangsidentifikationscode ($IMSI_c \neq IMSI_s$) die Terminaleinheit (1) und die Zugangseinheit (2) durch Eingeben entweder des Terminal-Identifikationscodes (PIN_t) oder des zweiten Zugangseinheits-Identifikationscodes (PIN_c) entriegelt werden.

6. Vorrichtung nach einem der Ansprüche 1, 2 oder 4, dadurch gekennzeichnet, daß bei Nichtübereinstimmung zwischen tatsächlichem und einem gespeichertem Zugangsidentifikationscode ($IMSI_c \neq IMSI_s$) der Terminal-Identifikationscode (PIN_t) und der zweite Zugangseinheits-Identifikationscode (PIN_c) eingegeben werden müssen.

7. Vorrichtung nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß die Terminaleinheit (1) ein Mobiltelefon umfaßt.

8. Vorrichtung nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß die Zugangseinheit (2) ein Karte umfaßt, beispielsweise mit einem elektronischen oder magnetischen Speicher.

9. Vorrichtung nach Anspruch 8, dadurch gekennzeichnet, daß die Zugangseinheit (2) eine SIM-Karte (Subscriber Identity Module) umfaßt, die die Teilnehmeranmeldung des Mobiltelefons (1) definiert.

10. Vorrichtung nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß der erste Zugangseinheits-Identifikationscode ($IMSI_{c,i}$) für mindestens eine Teilnehmeranmeldung, die Zugang zu der Telefoneinheit (1) oder der Terminaleinheit haben sollte, in der Terminaleinheit gespeichert ist, welcher Identifikationscode beispielsweise in einem EEPROM-Speicher in an sich bekannter Weise vollständig, teilweise, verschlüsselt, als Zufallszahl mit Rest etc. gespeichert ist.

11. Vorrichtung nach Anspruch 10, dadurch gekennzeichnet, daß ferner ein oder mehrere weitere Zugangseinheits-Identifikationscodes ($PIN_{c,i}$) in einem Speicher in der Terminaleinheit (1) beispielsweise vollständig, teilweise oder verschlüsselt in einer an sich bekannten Weise gespeichert sind.

12. Vorrichtung nach Anspruch 11, dadurch gekennzeichnet, daß mindestens ein zweiter Identifikationscode ($PIN_{c,i}$) in einem Speicher in der Terminaleinheit (1) verschlüsselt gespeichert ist.

13. Vorrichtung nach einem der Ansprüche 10 - 12, dadurch gekennzeichnet, daß die Speicherung des ersten Zugangsidentifikationscodes ($IMSI_s$) automatisch erfolgt.

14. Vorrichtung nach einem der Ansprüche 10 - 12, dadurch gekennzeichnet, daß die Speicherung des ersten Zugangsidentifikationscodes ($IMSI_s$) manuell erfolgt, beispielweise mittels einer Drucktasteneinrichtung (5) oder auf ähnliche Weise.

15. Vorrichtung nach einem der Ansprüche 10 - 14, dadurch gekennzeichnet, daß mindestens ein zweiter Zugangsidentifikationscode (PIN_c) in einem Speicher in der Terminaleinheit (1) in einer Weise gespeichert ist, die im wesentlichen analog zu der Speicherung des ersten Zugangsidentifikationscodes ($IMSI_s$) ist.

16. Vorrichtung nach einem der Ansprüche 7 - 15, dadurch gekennzeichnet, daß mindestens eine zu mindestens einer Zugangseinheit (2) gehörende Telefonnummer entweder in einem Terminalspeicher oder in einem Speicher in der Karte gespeichert ist, so daß sie aus dem Speicher aufgenommen und auf einer Anzeige (6) angezeigt wird, wenn die Vorrichtung (10) entriegelt ist.

Revendications

1. Ensemble (10) destiné à rendre des services tels

que des communications téléphoniques, des communications de données, etc., comprenant une unité terminale (1) et une unité d'accès (2), l'unité terminale (1) comprenant un dispositif (PIN_i) d'identification d'unité terminale mémorisé dans l'unité terminale (1) et l'unité d'accès (2) comprenant un premier dispositif (IMSI) d'identification d'unité d'accès sous forme d'un code ou analogue, l'unité terminale (1) et l'unité d'accès (2) pouvant être verrouillées, caractérisé en ce que, dans l'unité terminale (1) sont en outre mémorisés un premier dispositif d'identification d'unité d'accès ($IMSI_{s,i}$) pour un nombre donné (n) d'unités d'accès (2) (SIM) et en ce que l'unité d'accès (2) comporte un second dispositif d'identification d'unité d'accès (PIN_c) qui peut être activé ou inactivé, et, après le lancement du fonctionnement de l'ensemble qui comprend la mise en contact de l'unité terminale (1) et de l'unité d'accès (SIM) (2) avec certains dispositifs d'identification d'unité d'accès ($IMSI_c$), le code du dispositif d'identification ($IMSI_c$) de l'unité d'accès (2) est comparé à un ou plusieurs codes mémorisés dans l'unité terminale pour les dispositifs d'identification d'unités d'accès ($IMSI_{s,i}$), dans lequel la correspondance entre le premier dispositif mémorisé d'identification d'unité d'accès ($IMSI_{s,i}$) et le premier dispositif réel d'identification d'unité d'accès ($IMSI_c$) provoque un verrouillage de l'unité terminale (1), alors que, en l'absence de correspondance entre les premiers dispositifs d'identification d'unités d'accès mémorisé et réel, l'unité d'accès (2) et l'unité terminale (1) sont déverrouillées lorsque l'utilisateur donne un code correspondant au dispositif d'identification d'unité terminale (PIN_l) et un code correspondant au second dispositif d'identification d'unité d'accès (PIN_c) en cas d'activation.

2. Ensemble selon la revendication 1, caractérisé en ce que le second dispositif d'identification d'unité d'accès (PIN_c) comporte un code qui est donné manuellement par l'utilisateur.

3. Ensemble selon la revendication 1, caractérisé en ce que le second dispositif d'identification d'unité d'accès aussi (PIN_c) est mémorisé dans l'unité terminale (1), l'unité terminale, lors de la correspondance entre les codes mémorisé et réel d'identification d'accès ($IMSI_s = IMSI_c$), transfèrant automatiquement le second dispositif d'identification (PIN_c) à l'unité d'accès (2) afin que l'ensemble (10) puisse être utilisé sans le second code d'identification d'unité d'accès (PIN_c) qui doit être donné par l'utilisateur.

4. Ensemble selon la revendication 1, caractérisé en ce que, si le second dispositif d'identification d'unité d'accès (PIN_c) n'a pas été mémorisé et en cas de correspondance entre le premier dispositif d'identification d'unité d'accès ($IMSI_{s,i}$) mémorisé dans l'unité terminale (1) et le dispositif réel d'identification d'unité d'accès ($IMSI_c$), l'unité d'accès (2) est verrouillée par saisie de (PIN_c).

5. Ensemble selon la revendication 1, caractérisé en ce que, en cas de défaut de correspondance entre les codes mémorisé et réel d'identification d'accès ($IMSI_c \neq IMSI_s$), l'unité terminale (1) et l'unité d'accès (2) sont déverrouillées par transmission du code d'identification de terminal (PIN_l) ou du second code d'identification d'unité d'accès (PIN_c).

6. Ensemble selon l'une quelconque des revendications 1, 2 et 4, caractérisé en ce que, en cas de défaut de correspondance entre les codes réel et mémorisé quelconques d'identification d'accès ($IMSI_c \neq IMSI_s$), le code d'identification de terminal (PIN_l et un second code d'identification d'accès (PIN_c) doivent être donnés.

7. Ensemble selon l'une quelconque des revendications précédentes, caractérisé en ce que l'unité terminale (1) est un téléphone mobile.

8. Ensemble selon l'une quelconque des revendications précédentes, caractérisé en ce que l'unité d'accès (2) comporte une carte, par exemple avec une mémoire électronique ou magnétique.

9. Ensemble selon la revendication 8, caractérisé en ce que l'unité d'accès (2) comprend une carte SIM (module d'identification d'abonné) qui détermine l'abonnement du téléphone mobile (1).

10. Ensemble selon l'une quelconque des revendications précédentes, caractérisé en ce que le premier code d'identification d'unité d'accès ($IMSI_{c,l}$) d'au moins un abonnement qui devrait avoir accès à l'unité téléphonique (1) ou à l'unité terminale est mémorisé dans l'unité terminale, le code d'identification étant mémorisé par exemple dans une mémoire EEPROM d'une manière connue, sous forme d'un numéro complet, partiel, chiffré, aléatoire créé avec le reste, etc.

11. Ensemble selon la revendication 10, caractérisé en ce qu'en outre un ou plusieurs codes supplémentaires d'identification d'unité d'accès ($PIN_{c,i}$) sont mémorisés dans la mémoire de l'unité terminale (1) par exemple sous forme entière, partielle ou chiffrée de toute manière connue.

12. Ensemble selon la revendication 11, caractérisé en ce qu'un second code d'identification au moins ($PIN_{c,i}$) est mémorisé sous forme chiffrée dans une mémoire de l'unité terminale (1).

13. Ensemble selon l'une quelconque des revendications 10 à 12, caractérisé en ce que la mémorisation du premier code d'identification d'accès ($IMSI_s$) s'effectue automatiquement.

14. Ensemble selon l'une quelconque des revendications 10 à 12, caractérisé en ce que la mémorisation du premier code d'identification d'accès ($IMSI_s$) est réalisée manuellement, par exemple par un dispositif à bouton-poussoir (5) ou analogue.

15. Ensemble selon l'une quelconque des revendications 10 à 14, caractérisé en ce qu'un second code d'identification d'accès au moins (PIN_c) est mémorisé dans une mémoire de l'unité terminale (1) d'une manière essentiellement analogue à la mémorisation du premier code d'identification d'accès ($IMSI_s$).

16. Ensemble selon l'une quelconque des revendications 7 à 15, caractérisé en ce que l'une au moins d'au moins une unité d'accès (2) appartenant à un numéro téléphonique est mémorisée, soit dans une mémoire du terminal, soit dans une mémoire de la carte afin qu'elle soit déterminée dans la mémoire et représentée sur un dispositif d'affichage (6) lorsque l'ensemble (10) est déverrouillé.

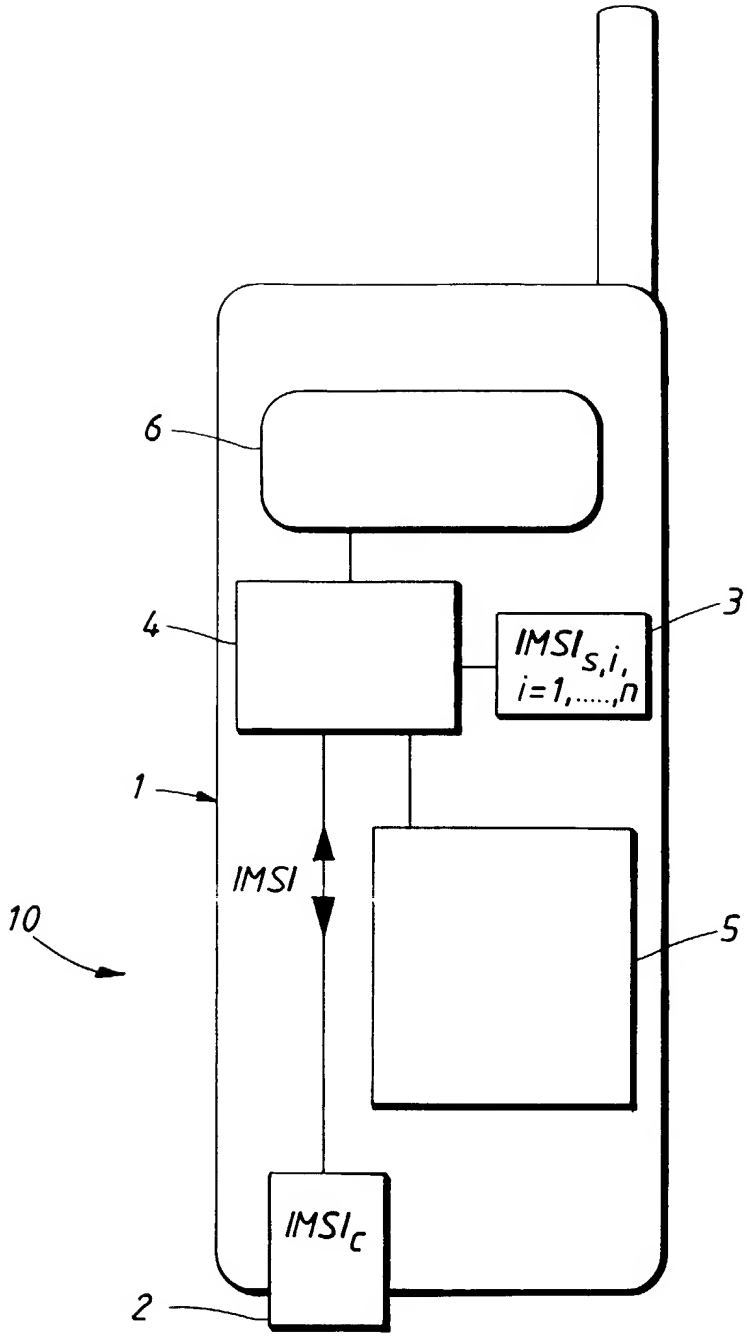

FIG. 1

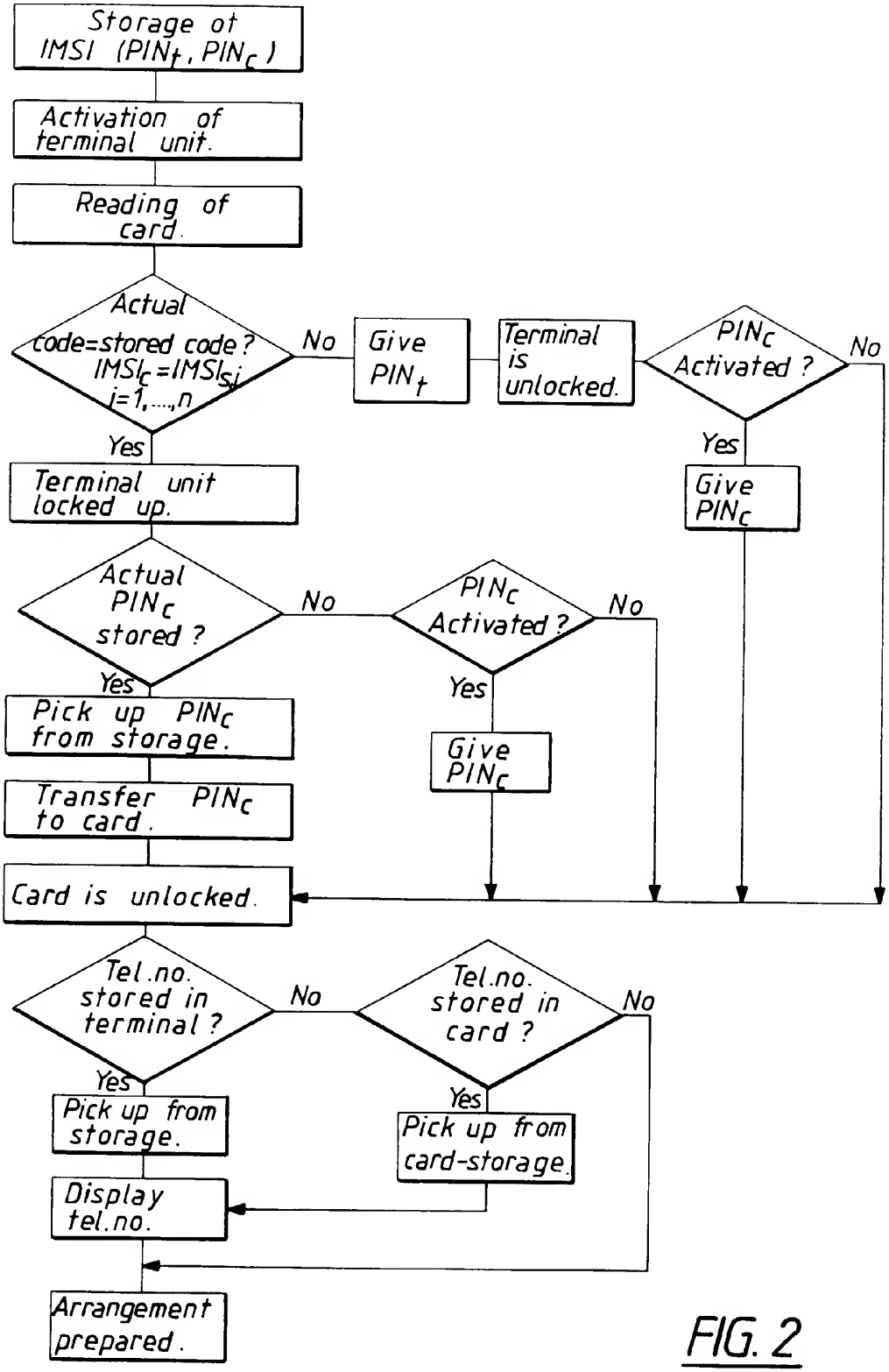
Storage of IMSI (PIN$_t$, PIN$_c$)
Activation of terminal unit.
Reading of card.
Actual code=stored code? IMSI$_c$=IMSI$_{si}$ i=1,....,n
No
Give PIN$_t$
Terminal is unlocked.
PIN$_c$ Activated ?
No
Yes
Give PIN$_c$
Yes
Terminal unit locked up.
Actual PIN$_c$ stored ?
No
PIN$_c$ Activated ?
No
Yes
Pick up PIN$_c$ from storage.
Yes
Give PIN$_c$
Transfer PIN$_c$ to card.
Card is unlocked.
Tel.no. stored in terminal ?
No
Tel.no. stored in card ?
No
Yes
Pick up from storage.
Yes
Pick up from card-storage.
Display tel.no.
Arrangement prepared.

FIG. 2